




Summary and Resources

Summary and Resources



Course Credit & Download page as a PDF

Download this page as a PDF  for quick reference. For course credit, look for the "Feedback and Credit" button at the bottom of the page or go to our [Credit SEC 0201](#) page now.


Your Cyber Security Responsibility and Requirements

You're responsible for the cyber security of computers and devices that you use or manage - plus the information that is stored on them. Make sure that you meet our [Minimum Security Requirements](#) . Don't hesitate to contact your line manager, [Computer Security Liaison](#)  (password protected), or Cyber Security Operations at security@lbl.gov.













Top threats: What to do and what not to do

Top Threats	Do	Do not
Loss of PII	<ul style="list-style-type: none">If you see Personally Identifiable Information (PII) anywhere it does not belong, report it to security@lbl.gov<ul style="list-style-type: none">If you wish to report PII and remain anonymous, we can support that requestIf you work with PII, review our Protected Information Requirements If you are involved in any process that may involve PII, contact security@lbl.gov and we'll help you develop the best controls and securityDefinition of PII: Social Security Number, Driver's License #, Financial Account Data, Individual identifier PLUS any type of health information	<ul style="list-style-type: none">Do not store PII on your computer, external hard drives, or mapped drives such as H: T: or V:Do not email PII.Do not store PII outside of HRIS or FMS, the institutional systems for human resources and financial data.Do not store paper collection of PII unless approved by Cyber Security Operations.
Spam and Phishing Attacks	<ul style="list-style-type: none">Report targeted spam or phishing to security@lbl.govFor normal spam or phishing (not targeted), use your email client to flag it as spamVerify web and email addresses (e.g. make sure it's a .gov, not .com)Be wary of vague messages or references to new or unknown projectsWhen viewing an email think, "could this be an attack?"	<ul style="list-style-type: none">Do not open attachments you are not expectingDo not click on links in emails you are not expectingDo not provide your username or password or any other account information via emailDo not download a file that ends in .exe
Drive-by Downloads	<ul style="list-style-type: none">Check your browser plugins using go.lbl.gov/browsercheck PCs & Macs: Install BigFix on your work computerSet up auto updates for your operating system and applications when possibleInstall Antivirus software. Sophos is available for Berkeley Lab and home usage at software.lbl.gov	<ul style="list-style-type: none">Do not use Internet Explorer, except when required for business applications like FMSDo not ignore update notifications from your OS, browser, and third parties like AdobeDo not use old browser versions





Tools, Software, and Services

Throughout the course, we mention a variety of tools - here they are, all in one place. You can also visit [the Cyber Security website](#)  for more information and resources.


Tool, Software, or Service	Description	Link to Resource(s)
----------------------------	-------------	---------------------

BigFix & Qualys BrowserCheck	BigFix will automatically patch Java and Flash plugins for PCs and Macs (only use for your work computer). Qualys BrowserCheck will check all of your plugins on any browser to see if any need to be updated (use for work and personal computers).	<ul style="list-style-type: none"> Instructions on installing BigFix & using BrowserCheck  Use Qualys now at go.lbl.gov/browsercheck 
Network blocks	Vulnerable computers are blocked from network access	<ul style="list-style-type: none"> Check for blocks at onestop.lbl.gov 
Sophos Anti-Virus	This is the cyber security team recommended Anti-Virus software. Available for Macs and PCs for work and home computers if used for work.	Download Sophos at http://software.lbl.gov  . Look under the Security Software section. Installation instructions available here: https://commons.lbl.gov/display/itfaq/AntiVirus 
Change your Password Service	Use our password change service when required or when you have any reason to believe that your password has been compromised.	https://password.lbl.gov/ 
Backup Services	Berkeley Lab offers a number of services for backing up data.	https://commons.lbl.gov/display/itdivision/Backups 
Report theft of a mobile device	If any IT asset is lost or stolen, you should report it immediately using our form.	https://commons.lbl.gov/display/cpp/Report+Lost+or+Stolen+IT+Assets 
Identity Finder	This software searches your computer to identify any potential PII. Available for PCs and Macs.	<ul style="list-style-type: none"> Instructions on using Identity Finder: https://commons.lbl.gov/x/ZwDeB  Download Identity Finder at http://software.lbl.gov . Look under the Security Software section.
OTP - One Time Password Service	If you use SSH, consider using this free service. Available for Microsoft Windows, OSX and Linux	Instructions to obtain OTP: go.lbl.gov/otp 
Central Syslog	Macs and Linux/Unix systems must syslog to the central syslog server. Exemption: Do not syslog to the central syslog server if your computer is offsite or frequently offsite (e.g. a laptop).	Instructions for the central syslog: https://commons.lbl.gov/display/cpp/LBNL+Central+Syslog+Server 

Additional Training

Training	Description	Link
Privacy and Protected Information Training	This training is required for employees that use or access PII. However, all employees are welcome to take it.	Protected Information Training (SEC 0220) 
Social Engineering	Spam and phishing rely on "social engineering" to trick you into clicking on that link or opening that bad attachment. You can read more about social engineering including other methods, e.g. telephone, media (CD's, DVD's, USB sticks), and the web.	Social Engineering - More Examples 
Spam and Phishing - More examples	Read about more examples of targeted attacks at Berkeley Lab.	Spam, Phishing, and Hoaxes 
Video - Advanced training on Targeted Phishing	Learn more about how we've been targeted and how you can prevent it.	View our video on targeted phishing.  (s croll to bottom of page)

Policies & Procedures

You can read more about all cyber-related RPM policies and procedures at our [IT policy page](#) .

Download page as a PDF

[Download this page as a PDF](#)  for quick reference.